

REMARKS

Claims 11-30 are pending in the application after entry of this amendment. Claim 11 stands objected to under 35 U.S.C. §112 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 11-14 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,768,390 to Coppersmith et al. in view of U.S. Patent No. 6,330,675 to Wiser et al. For the reasons set forth below, reconsideration of the amended application is respectfully requested.

First as to the objection under §112, it is respectfully submitted that the term “the immediately preceding encryption/decryption module” finds antecedent basis in the requirement of the claim that the at least three encryption/decryption modules must be arranged in series. One consequence of arranging the modules in series is that each intermediate and the last module must each have an immediately preceding module. Reconsideration of the §112 objection is respectfully requested.

As to the rejection under §103, one significant difference between the claimed invention and the processes described by the cited prior art is that with the claimed invention a packet of data goes first into a first encryption/decryption module which starts to encrypt/decrypt the data and, before that encryption/decryption process is complete, a second encryption/decryption module begins operating on the (partial) result of the first module. In contrast, with the cited prior art a packet of data similarly goes to a first encryption/decryption module which begins encrypting/decrypting the data, but in the prior art system the second encryption/decryption module does not receive any of the data from the first encryption/decryption module until the first module has completed it's

work on the packet. This distinction is believed to be stated by the language of claim 1 which states that each intermediate and the last encryption/decryption module (different from the first module) begins encryption/decryption operations before the immediately preceding encryption/decryption module has terminated its encryption/decryption operation. Since that feature is neither taught nor suggested by the cited prior art, the §103 rejections should be withdrawn.

Addressing more specifically the cited prior art, U.S. Patent No. 5,768,390 to Coppersmith is believed to describe a method for encrypting and masking data blocks with cascaded modules. An input data block is encrypted by a first module with a first key and combined with a first secret masking value to generate a masked first encryption product. The latter is encrypted and masked by a second module with a second key to generate a second encrypted and masked product and so on according to the number of modules.

As indicated above, one difference between Coppersmith and applicant's claimed invention is that in Coppersmith the operations are performed sequentially, (see col. 3, lines 29-47). That is, each module operates with the complete result of the preceding module. A module from the chain does not start operating before the preceding one has terminated. In all the embodiments described in Coppersmith there is no indication that a module begins to work when it receives partial results from the preceding module. In contrast, in the claimed invention each module after the first module begins its operations before the immediately preceding module has terminated its operation.

In U.S. Patent No. 6,330,675 to Wiser a device for securely decrypting and writing an encrypted digital file to a local storage medium is disclosed. The device

includes a first decryption engine, a first local memory, an encryption engine, a local storage medium, a second decryption engine and a second local memory. The first decryption engine incrementally decrypts the encrypted digital file in portions in order to prevent that the whole file is stored in a decrypted form. These portions may be decompressed and buffered by the first local memory. The encryption engine then re-encrypts the decrypted portions from the first local memory to form an intermediate file, which is stored in the local storage medium. The second decryption engine incrementally decrypts the intermediate file, buffering the decrypted portions in the second local memory until they can be written to a recordable storage medium. Accordingly, Wiser does not disclose a method of encryption and decryption carried out by at least three encryption/decryption modules arranged in series, wherein each intermediate and the last encryption/decryption module begins encryption/decryption operations before the immediately preceding encryption/decryption module has terminated its encryption/decryption operation.

Further, the device and method described by Wiser use RC4 or DES algorithm known as working with symmetric keys. See col. 4, lines 62 to 67. No other algorithm such as RSA using asymmetric keys (public and private keys) is mentioned in the document.

Similarly, the method described in Coppersmith document uses also encryption/decryption algorithms using symmetrical keys (DES), each module operating with the complete result of the preceding one.

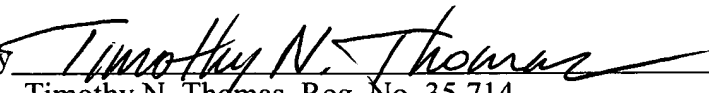
Accordingly, the combination of Coppersmith and Wiser documents does not teach or suggest applicant's claimed invention because, inter alia, the

encryption/decryption of the cited prior art is carried out with symmetric keys only in all modules. In applicant's claimed invention asymmetric keys, including a private key and a public key, are used.

As to new claims 21-30 which have been introduced by this amendment, those claims have been added to more particularly point out and distinctly claim certain aspects of applicant's disclosed invention. The subject matter of those claims is believed to be disclosed in the application as filed, and no new matter is believed to have been added by the claims.

In view of the above it can be seen that the cited prior art fails to teach or suggest a method wherein the security of the system is guaranteed both by using chained operations where at least three encryption/decryption modules are arranged in series, with each intermediate and the last encryption/decryption module beginning its encryption/decryption operations before the immediately preceding encryption/decryption module has terminated its encryption/decryption operation, and by using an asymmetric key algorithm, including a private key and a public key, in at least one module of the chain. The pending claims require both of those features. Reconsideration of the rejection under §103 is therefore respectfully requested.

Respectfully submitted:

By 
Timothy N. Thomas, Reg. No. 35,714
Woodard, Emhardt et al. LLP
111 Monument Circle, Suite 3700
Indianapolis, Indiana 46204-5137
(317) 634-3456